UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/107,618	06/30/1998	STEVEN M BLUMENAU	E0295/7066RF	8313

	7590	04/21/2006

WOLF GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2211

EXAMINER
DINH, DUNG C

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	09/107,618	BLUMENAU ET AL.
Office Action Summary	Examiner	Art Unit	
	Dung Dinh	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 December 2005</u>.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-4,6-27 and 29-34</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-4,6-27 and 29-34</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
        1.☐ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>12/23/05</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/23/05 has been entered.

Response to Arguments

Applicant's arguments filed 12/23/05 have been fully considered but they are not persuasive with respect to Ericson and Yu.

Regarding the rejection of claims 1, 15 and 21 under Eustace, the argument is persuasive. The rejection is withdrawn.

Regarding the combination of Ericson and Yu, Applicant argued essentially that Ericson system is in a trusted environment - each node is trusted not to proof the identity of another node; hence Ericson system does not need the node authentication security of Yu. Applicant argued therefore there is no motivation to combine Yu with Ericson.

Applicant asserted that Ericson system is a trusted

environment because it uses SCSI bus that has limited number of

nodes and manually assignment of node ID's. Applicant point out

specific details of the SCSI bus specification and concluded

that nodes in a SCSI bus cannot spoof the identity of another

node.

Assuming Applicant's characterization of the SCSI bus is

correct, the argument is still not persuasive because the usage

of the SCSI bus is only a preferred embodiment. Ericson

specifically stated that his invention is applicable to other

protocols such as Fibre Channel. (See col.6 lines 1-6).

It is well known in the art at the time of the invention

that SCSI peripherals may be distributed over wide area network

using ATM and Fibre Channel. (See for example Boggs et al. US

patent 5,959,994 col.2 lines 63-68, col.10 lines 8-22).

Hence, the argument that Ericson operates only in a trusted

environment is not commensurate with Ericson disclosure.

Yu discloses that distributed network is venerable to

identity spoofing (col.4 lines 56-65). Yu specifically

discloses that security based on access control only is

inadequate (col.1 lines 60-63, col.2 lines 7-10). Hence, Given

the teaching of Yu, one of ordinary skill in the art would have

been motivate to use both the access control security of Ericson

together with authentication security of Yu to form an enhanced

security system to prevent both unauthorized access and

identification theft.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. § 103(a) which
forms the basis for all obviousness rejections set forth in this
Office action:

> *(a) A patent may not be obtained though the invention is
> not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject
> matter pertains. Patentability shall not be negatived by
> the manner in which the invention was made.*

Claims 1-4, 9-27, 29-32 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Ericson US patent 6,061,753 and

further in view of Boggs et al. US patent 5,959,994 and Yu US

patent 4,919,545.

As per claim 1, Ericson teaches a data management method

for managing access to a storage system between two devices

coupled to the storage system through a network [col.1 "SCSI

Fibre Channel bus or Ethernet based local area network"], the

method comprising:

Receiving over the network at the storage system a request

from one of the device [initiator - see col.3 lines 56-60];

Selectively servicing, at the storage system, the request

responsive to configuration data indicating that the device

[initiator] is authorized to access the portion of data [col.4

lines 4-25].

Ericson does not teach authenticating the request at the

storage system to authenticate the device issuing the request. Yu

teaches a security method for authorizing access by a process in

source node to a resource in the network comprising encrypting an

identifier of the requesting node using a key associated with the

node, sending the encrypted key to the resource, decrypting the

identifier at the resource node to verify the request [see

abstract].

It is well known in the art at the time of the invention

that SCSI peripherals may be distributed over wide area network

using ATM and Fibre Channel. (See Boggs et al. US patent

5,959,994 col.2 lines 63-68, col.10 lines 8-22). Ericson

specifically discloses that his invention is applicable to Fibre

Channel protocols (col.6 lines 1-6). Hence, it would have been

obvious for one of ordinary skill in the art to combine Boggs

and Ericson because it would have enabled distributed access

control to peripherals over wide area network.

Yu discloses that distributed network is venerable to

identity spoofing (col.4 lines 56-65). Yu specifically

discloses that security based on access control only is
inadequate (col.1 lines 60-63, col.2 lines 7-10). Hence, Given
the teaching of Yu, one of ordinary skill in the art would have
been motivate to use both the access control security of Ericson
together with authentication security of Yu to form an enhanced
security system to prevent both type of security breaches:
unauthorized access and identification theft.

Therefore, it would have been obvious for one of ordinary
skill in the art to combine the teaching of Yu with the storage
system of Ericson as modified to authenticate that the represented
device is the device making the request because it would have
prevented access by a device masqueraded as an authorized device
(see Yu col.3 line 29-35).

As per claim 2, Ericson teaches the storage system stores a
plurality of volumes of data where configuration data stored in
the storage system in a configuration table [look-up table]
having identifier and information indicating which volumes are
available to a device [col.4 lines 34-54].

As per claim 3, it is apparent Ericson as modified that the
request would be forwarded to the storage system over the
network.

As per claim 4, Ericson teaches using Fibre Channel [col.1 line 15, col.6 line 5]. It is apparent that a system with Fibre Channel would use Fibre Channel protocol.

As per claims 15-18, 21-22, 26-27 they are rejected under similar rationales as for claims 1-4 above. It is apparent that the process as modified would have computer program instruction stored on computer readable medium and the corresponding system for carrying out the method recited.

As per claims 11 and 30, Ericson teaches plural disk drives [RAID col.4 lines 5-15].

As per claims 12 and 29, Yu teaches validating that the request was not altered during transmit (col.3 lines 29-35).

As per claims 13 and 19-20, 24-25, Ericson teaches row with bitmap records corresponding to teach device authorized to access each of the corresponding ports [col.4 lines 40-53].

As per claims 14 and 23, Ericson teaches precluding service request responsive to configuration data [col.4 lines 47-50].

As per claims 9, 10, 31, 32, Ericson does not specifically disclose that the device is a host processor or file server. The type of device making the request would clearly have been a matter of design choice because it does not change the functionality of the storage system access control method taught by Ericson. Furthermore, Ericson teaches using the system may be used over a

local area network [col.1 lines 15-16]. Official notice is taken

that the usage of host processor and file server in a LAN or WAN

is ubiquitous at the time of the invention. Hence, it would have

been obvious host processor and file server requesting access to

the storage system in Ericson as modified in order to provide file

services to requesting clients.

**Claims 33, 6-8, and 34 are rejected under 35 U.S.C. 103(a)
as being unpatentable over Ericson, Boggs, and Yu, and further
in view of Abadi et al. US patent 5,315,657.**

As per claim 33, Yu teaches the request include a request

access key (capability + signature 44), and verify with an

expected key at the storage system (resource node) [see col. 6

line 50 to col. 7 line 44]. Yu does not teach sending an expected

access key between the storage system and the requesting device.

Yu teaches the resource node maintains a unique encryption key for

each requesting node [col.7 lines 12-15, lines 50-56]. Yu does

not specifically disclose how the resource node comes to

possession of these unique keys. However, the method of providing

encryption information to a destination node so that the

destination node can encrypt data specifically targeted for the

providing node is well known in the art. Abadi discloses using

RSA cryptography to authenticate the identity of a requesting node

by providing a public key to the destination and the destination returning to the requesting node data (i.e. the claimed expected access key) encrypted using that public key such that it can only be decrypted with the requesting node's private key. [See Abadi col.4 lines 50-68, col.5 lines 1 to col.6 line 8]. RSA cryptography is a well-known secured encryption standard and code fore implementing the encryption is readily available. Hence, it would have been obvious for one of ordinary skill in the art to modify Ericson and Yu to use RSA cryptography because it would have eased implementation of the encryption features and to ensure difficulty for unauthorized device to gain access via theft of the access key.

As per claim 6, Yu teaches verifying the identified source by comparing the requested key to the expected key (col.3 lines 20-28).

As per claim 7, Yu clearly teaches encrypting using key associated with the device [col.7 lines 14-15].

As per claim 8, it is apparent that the system as modified would decrypt the access key using a decryption key provided initially by the device (the pubic key).

As per claim 34, Abadi teaches transferring of encryption information between the storage system and the device (the

exchange of public key information [see Abadi col.4 lines 50-68,

col.5 lines 1 to col.6 line 8]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dung Dinh whose telephone number is (571) 272-3943. The examiner can normally be reached on Monday-Friday from 7:00 AM - 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached at (571) 272-3949.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Dung Dinh
Primary Examiner
April 14, 2006